There are three NAT-handling algorithms in Cisco IPSEC implementations:

1) NAT-T (travesal, udp:4500). NAT device is unaware of IPSec. NAT-D(iscovery) packets are included in third and fourth IKE-exchange in Main Mode and in second and third messages in Aggressive Mode of IPSec negotiation.

2) NAT over TCP (tcp:10000). NAT device is unaware of IPSec. Proprietary solution (Cisco ASA, VPN Concentrator, IOS have it).

3) NAT support for IPSEC ESP Phase II. Used as a last resort when the Port Address Translation is configured somewhere between IPSec peers and one or both IPSec peer doesn't support NAT-T or NAT over TCP. NAT device must be SPI-aware (Security Policy Index). Configuration needed on both peers and NAT device.

Note 1: Cisco IOS routers support NAT-T by default. As far as I remember you have to configure *crypto isakmp nat-traversal* in PIX/ASA 6.x/7.x (not sure about 8.x) to turn on NAT-T algorithm at PIX/ASA. In case of VPNC (if any still alive ;) you also have to find the right switch to turn NAT-T support on:).

RFC3715

Cisco IPSec technology support page , configuration examples

Feature Design of IPSec NAT Traversal aka NAT-T internals